# Our Requirements

# Information Governance & Controlled Documents

## Why is this important?

**Effectively managing records and information reduces risk, minimises costs and enables us to operate sustainably by maximising the value of information.**

Document control
This document is uncontrolled when printed or downloaded and should be discarded after use. Always source the most recent version from the White Rose *Governance Fundamentals Library* and share only the document link.

| | | |
|---|---|---|
| Document title | **Information Governance & Controlled Documents** | Verbatim of above |
| Identification | **OR008** | A unique identification number: letters followed by three digits. |
| Status | **Published** | The lifecycle status: draft/published. |
| Version | **1** | Major number only (0=draft; 1; 2; etc) |
| Approval Date | **26 February 2026** | The date this version of the document was approved |
| Revalidation Date | **26 February 2028** | The date the document is due for review. A maximum of two years after the approval date. |
| Approver | **Lee Mason** | Title of the person who owns and is responsible for the document |

| Revision History | | |
|---|---|---|
| Revised by | Revisions/changes/comments | Date re-published |
| Lee Mason | **First drafting** | |
| | | |
| | | |
| | | |

## Table of Contents

## 1. Information Governance

When managing information:

- Have a retention and disposal schedule and apply it (see Appendix 1).
- Apply the Information Protection Framework (IPF) (see Appendix 2) by:
    - Assigning an appropriate IPF classification.
    - Applying the information labelling and handling requirements.
- Notify the Director/Founder immediately if information classified as *Confidential: White Rose* or *Confidential: Personal* (or higher in the case of Government) is lost or disclosed to unauthorised parties; or is suspected of being lost or disclosed to unauthorised parties.

## 2. Managing Personal Information

When managing personal information (examples may include names, location data, email addresses, photographs, job applications, banking information, etc.):

- Comply with the privacy principles (see Appendix 3)
- Contact the Director/Founder immediately if you become aware of any suspected or confirmed unauthorised disclosure of, misuse, or access, to personal information.

## 3. Controlled Document Management

A controlled document is an Our Requirement, Procedure/Guide, Form, or Work Instruction that requires periodic review – see Appendix 4 for descriptions.

When creating a new or reviewing an existing controlled document:

- Only create a controlled document to meet legislated requirements, control a risk, or significantly improve efficiency and effectiveness.
- Keep it short and simple.
- Do not duplicate or contradict Our Requirements.
- Categorise the document as per Appendix 4.

## Appendix 1 - Retention and disposal framework

The following table sets out retention periods and a list of types of records. Apply these, unless otherwise required by law.

| Retention period | Type of information/subject | Description |
|---|---|---|
| **3 years or less** (dispose of this information as soon as it is no longer required. Do not keep for more than three years.) | Non-records | Information with no ongoing business value or legal requirement to retain. |
| | Recruitment or Expressions of Interest | Job applications resume, interview notes, criminal background checks, pre-employment medical checks, unsuccessful job candidates. |
| | Business contact information with no ongoing business relationship | Contact information (e.g., name, email, address, job title) of individuals with no ongoing business relationship with White Rose. |
| **7 years** (after the last action, unless otherwise stated) | Outputs of Our Requirements | Final versions of outputs mandated by Our Requirements. |
| | Finance | Evidence of processes or outcomes in support of Taxation or Financial Statements. |
| | HSEC | Documentation for risk, incidents, or regulator reporting. |
| | Employment records | Retain for the duration of employment, plus 7 years:<br>-Disciplinary notes<br>-Records relating to sick leave and absence<br>-Hiring records<br>-Induction records<br>-Payroll processing<br>-Medical files |
| | Legal | Advice, executed contracts |
| | Risk and assurance | Risk assessments, Insurance policies, claims, audit records. |
| | Technology | Outcomes of cybersecurity investigations. |
| **Permanent** (do not dispose of these records unless otherwise stated) | Board | Board submissions, papers, agendas, meeting minutes and resolutions. |
| | Entities | Company financial statements, share certificates, and company deeds. |
| | Controlled documents | Our Requirements, Processes or Guidance, and Project SOPs. |

## Appendix 2 – Information Protection Framework

The information Protection Framework (IPF) guides the protection of information from risks including, but not limited to loss, unauthorised disclosures, access, use, modification, and removal.

The IPF applies to all information created and owned by White Rose, whether handled by employees, contractors, vendors, suppliers, third-party service providers or their staff, regardless of the information's medium or format.

**Category definitions**

The following table sets out categories and definitions; by doing this, we protect our intellectual property, reputation, and assets.

| | Public | Confidential |
|---|---|---|
| **The potential impact of the of breach** | Tolerable<br>(A or B in our Risk Rating) | Unacceptable<br>(C or D in our Risk Rating) |
| **Definition** | No adverse impact on White Rose if the information is made available beyond our employees and selected external people. | Information that, if disclosed or made available beyond White Rose employees and selected external people, could result in a serious or major disruption to White Rose.<br><br>Examples may include:<br>- White Rose Confidential information.<br>- Personnel Information. |
| **Requirements when creating information** | Nil | Label either:<br>Confidential: White Rose<br>or<br>Confidential: Personal |

**Information labelling and handling requirements**

Apply the following labelling and handling requirements through the lifecycle of the information.

| | Public | Confidential (Confidential: WHITE ROSE, or Confidential: Personal) |
|---|---|---|
| **Printing / Fax information: documents are not disclosed to unauthorised personnel during the process** | | |
| Printing | Nil | - Use printers in secure areas.<br>- If unable, stay at the printer and remove the print out immediately. |
| Fax | Nil | - To and from company-controlled fax machines only. |
| **Sending physical information: physical information is transferred only to the appropriate recipient(s)** | | |
| Sending hardcopy documents | Nil | - May be sent through postal mail.<br>- Seal the document in a plain envelope with no classification markings. |
| Sending removable media (USB, | Nil | - May be sent through postal mail.<br>- Seal portable media in a plain envelope with no classification markings.<br>- Encrypt portable media. |

| | | |
|---|---|---|
| SD cards, etc.) | | |
| **Sending digital information: digital information is received and opened only by the appropriate recipient(s)** | | |
| Sending digital information (email, data transmission, etc.) | Nil | - Include IPF classification in the subject line of an email.<br>- Encrypt where practicable. |
| Telephones (voice calls) | Nil | - Only say what the other person, or those around you, ‘needs to know’. |
| **Storing information: physical and digital information is stored securely to prevent unauthorised disclosure or modification** | | |
| Storing physical information | Nil | - Clear documents from desks at the end of the day.<br>- Store in a secured location, restricted to authorised personnel. |
| Storing digital information | Nil | - [Primary] Store in a secured format (encrypted file), restricted to authorised personnel. If this is not practicable, then<br>- [Secondary] Store in a secure location (folder), restricted to authorised personnel.<br>- Conduct an annual review of users with access. |
| **Deleting/Destroying information: information is not kept for longer than required** | | |
| Destroying physical information | Nil | - Dispose in secure disposal bins, or<br>- Destroy in the shredder |
| Deleting digital information | Nil | - Permanently delete digital information no longer required (e.g., emptying Deleted Items folder / recycle bin) |

## Appendix 3 – Privacy Principles

- Categorise, label, and handle personal information per Appendix 2.
- Implement, as best as practicable, the privacy principles when using, disclosing, holding, recording, storing, transferring or otherwise handling personal information.

| Privacy principle | Description |
|---|---|
| **Privacy principle 1** | Have a legal, legitimate, and specific White Rose business purpose for collecting, using and sharing personal information and do not use it for any other purpose. |
| **Privacy principle 2** | Collect the minimum amount of relevant personal information for the specific White Rose business purpose, keep it accurate and up to date and dispose of it as soon as it is no longer required (per Appendix 1 as applicable). |
| **Privacy principle 3** | Tell individuals why their personal information is required and how it will be used. |
| **Privacy principle 4** | Let individuals exercise their legal rights to their personal information, for example, their right to access it, correct it, erase it, or object to it being used. |
| **Privacy principle 5** | Use technical and organisational measures to safeguard personal information against unauthorised or unlawful handling, use, sharing, loss, destruction or damage (including where third parties are processing personal information on White Rose's behalf). |
| **Privacy principle 6** | When transferring personal information from one country to another (whether inside or outside White Rose) make sure it is done lawfully. |

## Appendix 4 – Controlled document framework

| Controlled Document | Description |
|---|---|
| **Our Requirements** | Performance requirements and controls to achieve uniformity of a specific activity or process and support long-term requirements.<br>May be described in other organisation as ‘policy’ or ‘standard’. |
| **Procedure or Guide** | How to operate or control an activity or process to achieve required functionality, quality, and performance.<br>May be described in other organisation as ‘process’ or ‘handbook’. |
| **Form** | Documents with which users interact to create controlled outcomes.<br>May be described in other organisation as ‘template’ or ‘tool’. |
| **Work Instruction** | Documents which describe how to perform a task.<br>May be described in other organisation as ‘SOP’ or ‘wiki’. |
| **Why? Uniformity increases safety, repeatability, continuity, effectiveness and efficiency.** | |